Available online at https://www.ijasrd.org/

International Journal of Advanced Scientific Research & Development

Vol. 06, Iss. 03, Ver. I, Mar' 2019, pp. 24 – 33

e-ISSN: 2395-6089
p-ISSN: 2394-8906

SECURE VIDEO PROCESSING USING ROI EXTRACTION AND ECC ENCRYPTION

S. Aravindan[1*], R. Pavithra[2], J. Sindhuja[2] and R. Sobika[2]

[1] Asst. Prof., Department of Computer Science and Engineering, E.G.S. Pillay Engineering College, Nagapattinam.

[2] Final Year, Department of Computer Science and Engineering, E.G.S. Pillay Engineering College, Nagapattinam.

ARTICLE INFO

Article History:

Received: 18 Mar 2019;
Received in revised form: 29 Mar 2019;
Accepted: 29 Mar 2019;
Published online: 10 Apr 2019.

Key words:

Surveillance Video,
ROI Encryption,
Layered Cellular Automata,
Reversible Rule,
Shift Transformation.

ABSTRACT

Video encryption is the process of encrypting videos to hide the object in video for secure video sharing. To hide privacy from sensitive areas in video frame, ROI extraction techniques are proposed. Lightweight encryption algorithm is performed on every ROI to make the privacy sensitive information. To implement ECC encryption for encryption of extracted ROI. Provide secure video communication between sender and receiver.

INTRODUCTION

Network security is the security provided to a network from unauthorized access and risks. It is the duty of network administrators to adopt preventive measures to protect their networks from potential security threats.

With the rapid development of network and communication technology, the application of surveillance systems have significantly increased in the last two decades. Surveillance cameras are deployed not only in public places such as airport, bus station, but also in private places such as home, office, to name a few. By surveillance videos, the authenticated users can identify most of objects they want to observe or track with. For example, the users can see the live or stored surveillance videos on hand-held devices to know what is happening or has happened in their house. However, as it's possible to obtain the photos of humans' faces, the plate numbers of the cars among the monitoring area, the privacy information is then jeopardized through the surveillance cameras in public areas. The private places like homes are vulnerable to the surveillance videos too. Generally,

Cite this article as: Aravindan, S., Pavithra, R., Sindhuja, J., & Sobika, R., "Secure Video Processing using ROI Extraction and ECC Encryption". *International Journal of Advanced Scientific Research & Development (IJASRD), 06* (03/I), 2019, pp. 24 – 33. https://doi.org/10.26836/ijasrd/2019/v6/i3/60304.

*** Corresponding Author:** S. Aravindan, aravindan@egspec.org

encryption is an effective method to protect privacy as well as security. To hide privacy from sensitive areas, different cryptographic and ROI extraction techniques are presented. As a result, hardly is it integrated with an IOT device at the surveillance cameras' side.

Although video are made from frames, where each frame is an image with a compressed format, some inherent features such as redundancy, bulk data capacity and high correlation between pixels make the typical image cryptosystems unsuitable for videos.

PRELIMINARIES

A CA is a dynamic data handling framework whose space, time and state are for the most part discrete. The CA comprises of a few cells organized in a customary matrix. Every cell has its very own state and all cells refresh their states synchronously as per a presetting nearby principle. The new condition of a cell depends without anyone else state ever, yet additionally the conditions of its neighbors'. For a limited CA, the occasional limit conditions are generally connected, where the limit cells are linked as a falling framework and consequently the CA can be treated as a limited state machine.

For an1D CA, its nearby progress rule f is characterized as pursues:

Where s^t I indicates the condition of ith cell at time t and r is neighborhood range with the inside as s^t I. In the event that there are two cell states just, absolutely f has 22r+1 diverse data sources pursued by 222r+1 distinctive neighborhood change rules.

Basic CA (ECA) is the least difficult CA that every cell just has two conceivable states and three neighbors. There are 28 = 256 basic standards altogether and every one of them is listed by a whole number untruths in [0,255]. All conceivable info conditions of f are organized in the request as 111,110,• • • ,001,000, where the subsequent yield states framed a twofold succession and the relating rule number is spoken to by the picked decimal numbers. The model basic tenets are appeared in Table 1.

Table – 1: *Elementary Rule 15,30 and 90*

Rule	111	110	101	100	011	010	001	000
15	0	0	0	0	1	1	1	1
30	0	0	0	1	1	1	1	0
90	0	1	0	1	1	0	1	0

Reversible Cellular Automata (RCA) is a special case of CA whose transition rule is reversible and each state has only one successor and one predecessor. RCA is especially suitable for cryptosystem because the reversibility property of CA ensures that any encrypted message can be decrypted by the same algorithm performed in the reverse direction. It has been proved that whether a rule of an 1D CA is reversible is determined, whereas for a two or more dimension CA the same reversibility is un decidable. A layered cellular automata (LCA) is a cascading system of 2D CAs with the same size, where each layer is a composition of 1D CAs. The structure of LCAs makes a more complex but flexible expression ability.

In this paper, an 8-layer CA is devised by us to encrypt the RoIs of the gray surveillance video frames because the 8-layer CA can match up with the binary pixel matrix of a video frame completely.

THE FRAMEWORK OF OUR APPROACH

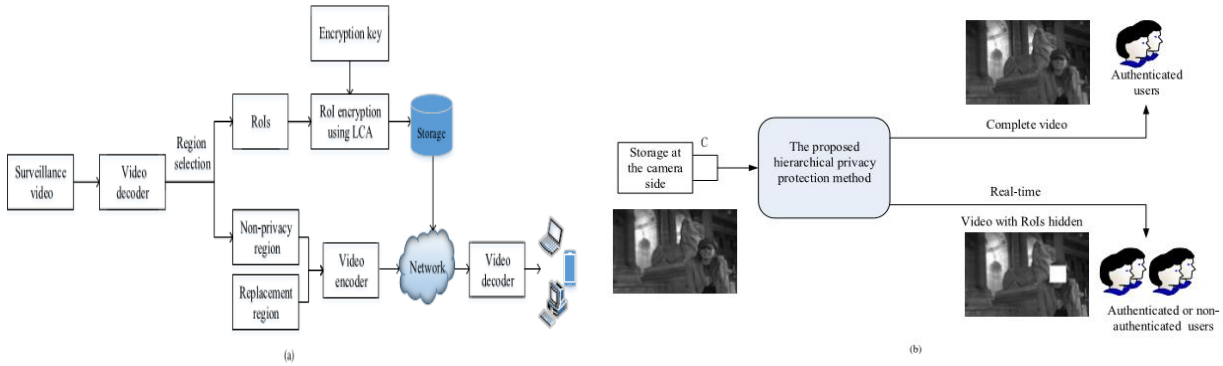
Our approach is a hierarchical privacy protection method for surveillance videos now can apply to the video format H.264. By our approach, the non-authenticated users can only see the real-time surveillance video without ROIs, while the authenticated users can watch the complete surveillance video through an on-demand manner.

The ROIs containing privacy sensitive information such as faces and license plates are extracted from the I frames (JPEG format) through the ROI detection and segmentation methods in. It's possible that there are more than one ROI in a video frame. The length and width of each ROI is the multiples of 16, so that each ROI can be divided into the sub-blocks of the size 16×16.

LCA based lightweight encryption algorithm is performed on every ROI to make the privacy sensitive information unrecognizable, and then all ROIs from a frame are encrypted independently. Hence, if there are some bits spoiled during the encoding and/or transmission, it will only affect the decryption within their blocks, which limits the errors propagation. All ROI blocks in a video frame are encrypted by the same random keys, which can reduce the consumption of the key's exchange and storage. Note that the ROIs from different video frames are required to use different encryption keys. After the ROIs are extracted, the pixel values with all (0 or 1) are filled back to replace the extracted ROI regions in the I frames. In what follow, the new surveillance video based on the new I frames is then re-encoded and transmitted, which can be watched real-time on a computer or a handheld device with network service. Whereas the encrypted ROIs are stored at the camera side without compression and be used for the on-demand service later, i.e., the stored ROI will be transmitted, decrypted and then integrated with the new I frames to recover the original surveillance video if and only if the authenticated users require to do so. Note that the encrypted ROI data lost almost all spatial correlations, compression cannot decrease the data size remarkably. The ROIs encryption and the new video's encoding are carried out independently, which make the proposed method can not only protect privacy information, but also meet the real-time requirement. In addition, since the ROIs in the original I frames are replaced with regions that pixel values are all 0 or 1, the surveillance video data compression ratio is increased because the correlations of these data are increased. The cost of our approach is the affordable delay for the authenticated users to retrieve the complete surveillance video.

ECC AND ROI ENCRYPTION ALGORITHM

- Propose a lightweight LCA-based method to encrypt the privacy sensitive ROIs for surveillance videos.
- It allows extending the existing surveillance systems without modifying the camera's hardware.
- It focuses on the ROI privacy protection with lightweight cryptographic techniques.
- Input video is convert into frames.
- To extract the ROIs from video frames is not highlighted.
- A ECC-based approach is devised to encrypt ROIs for privacy protection in surveillance videos.



(A) Key Generation

We first pick four sets of reversible ECA rules,{15,85}, {51,51}, {170,240}, and {204,204}, as the change guidelines, and afterward such principles are filed by a mapping capacity as following:

$$F : \{00, 01, 10, 11\} \rightarrow \{15/85, 51/51, 170/240, 204/204\}$$

Where F is an injective function. Furthermore, in each pair of rules, the one is utilized for encryption and the other is utilized for decoding. A pseudo arbitrary double succession PR is created from a seed number, which is secretly shared between the encryption and the decryption sides. The PR is divided into blocks of two bits, where each square speaks to a specific guideline for a 1D CA in the LCA. In this way, the length of the succession PR is controlled by the quantity of 1D CA in the LCA, where the number is decided by the height of its ROI block .specifically , the measure of a ROI square is 16×16, each layer of the layered CA has 16 lines and after that the length of the arrangement PR is 8×2×16=256. The double succession PR with the cycle number N will be utilized as the encryption and decoding key.

(B) Encryption

The ROI squares are scrambled as pursues.

Stage 1: Initialization. Arrange the binary sequence from the original RoI block into an 8-layerCA , and then let each layer contain 16×16 bits.

Stage 2: Rule advancement. Each layer is treated as a composition of the row shift the 1DCA switch the same size. There after, cells from different 1DCAs change their states independently according to different ECA rules which selected by the blocks in the succession PR.

Stage 3: Intra-layer move. A half move change is performed in each layer. For each line in a layer, just half cells change their states to the conditions of the cells at their adjoining line. specifically, the phones at back segments will change their states and alternate cells will keep static. In the event that there are k(k ∈ N+) segments in each layer, the condition of it

If there are $k(k \in N^{+})$ columns in each layer, the state of i^{th} row in the l^{th} layer at time t is $\left(S^{t}_{l,i,1},\cdots,S^{t}_{l,i,j},\cdots,S^{t}_{l,i,k}\right)$.

It will be shifted to the new state $\left(S^{t+1}_{l,i,1},\cdots,S^{t+1}_{l,i,j},\cdots,S^{t+1}_{l,i,k}\right)$ after an intra – layer half shift transformation, where

Note that such a change makes the half cells in each layer change their states , and it indirectly influences the cell snot shifted because such transformation can change their

neighbors' states. In this manner, if a cell in succession changes its state, it will influence the cells in indistinguishable column from well as in alternate lines.

Stage 4: Inter-layer move. It is a half move change between adjoining layers. Furthermore, this is an occasional change, where half cells in a single layer will move to its upper layer and the cells in the first layer will move to the last layer. Specifically, when the between layer half move change has occurred, the new conditions of the ith push in the lth layer is $(S_{l,i,1,\cdots}^{t+1}, S_{l,i,j,\cdots}^{t+1}, S_{l,i,k}^{t+1})$ at time t +1, where

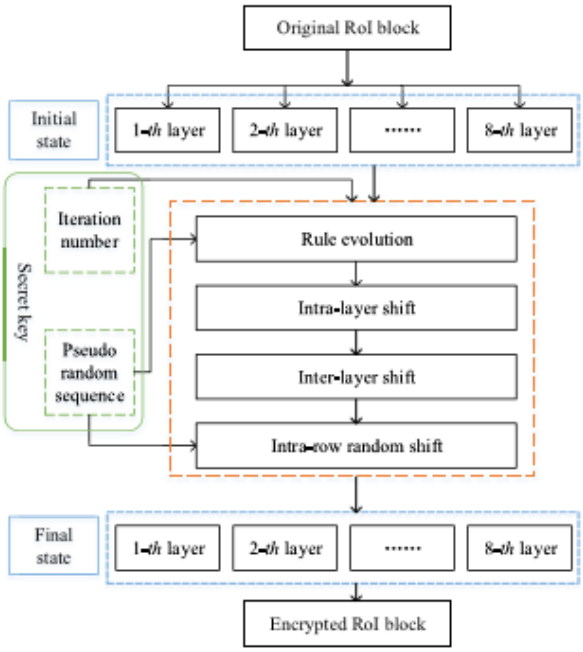
$$S_{l,i,j}^{t+1} = \begin{cases} S_{l+1,i,j}^{t}, 1 \le j \le \frac{k}{2} \\ S_{l,i,j}^{t}, \frac{k}{2} + 1 \le j \le k \end{cases}$$

Stage 5: Intra-push irregular move. Each 1D CA in a layer performs a periodic intra-row shift transformation. All cells in a1DCA shift to their left according to a random shift number. Give stomach muscle a chance to indicate the progress standard of a 1D CA selected by the parallel grouping in the key, where a,b ∈ {0,1}, at that point the move number of the CA is defined as a × 21 + b × 20 = 2a + b. Thusly, each 1D CA in the layered CA has four conceivable move numbers. Rehash Step 2 to Step 5 until the pre-defined cycle number came to. At long last, the scrambled ROI square is worked by changing over the final condition of the 8-layer CA into a pixel framework. Fig. 3 demonstrates the previously mentioned encryption process. Calculation 1 is utilized for ROIs encryption.

Table – 2: *Move Numbers with its Comparing Rule Lists*

Rule Index	11	10	00	01	00	10	11	10
Shift Number	3	2	0	1	0	2	3	2

Figure – 3: *The LCA-based Surveillance Video Encryption Algorithm*



Encryption Algorithm:-

– Suppose sender wants to send a message m to the receiver

- **Step 1:** Let m has any point M on the elliptic curve
- **Step 2:** The sender selects a random number k from [1,n-1]
- **Step 3:** The cipher texts generated will be the pair of points (B1,B2) where B1= k*G B2= M + (k*G)

(C) Decryption

The decoding key is equivalent to the encryption key. The advancement rules spoken to by the arrangement are the turn around principles of the ones utilized in the encryption. The binary sequence of an encrypted ROI block is set as the starting condition of a 8-layer CA. Forward moving uses the principles chosen by the decoding key. From there on, the converse changes of the three unique changes referenced above are performed, as well.

Figure – 4: *An Example of Random Shift*

1	0	0	0	0	1	1	0
1	0	0	1	1	0	1	0
1	1	0	1	1	0	0	0
0	1	1	0	1	1	0	0
0	1	0	0	0	1	0	1
0	1	1	0	1	1	0	0
0	1	0	0	1	1	1	1
1	0	0	0	1	1	0	1

(a)

→

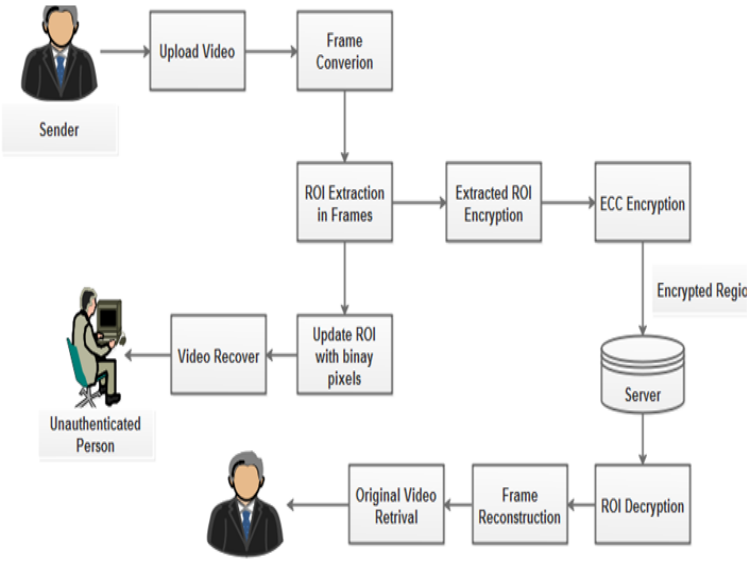
0	0	1	1	0	1	0	0
0	1	1	0	1	0	1	0
1	1	0	1	1	0	0	0
1	1	0	1	1	0	0	0
0	1	0	0	0	1	0	1
1	0	1	1	0	0	0	1
0	1	1	1	1	0	1	0
0	0	1	1	0	1	1	0

(b)

Decryption Algorithm

- To decrypt the cipher text, following steps are performed:-
  - **Step 1:** The receiver computes the product of B1 and its private key
  - **Step 2:** Then the receiver subtracts this product from the second point B2 M = B2- (dB * B1) M is the original data sent by the sender.

ARCHITECTURE



LIST OF MODULES

(a) Video Processing
(b) ROI Extraction
(c) ROI Encryption
(d) Video Retrieval

(a) Video Processing

- Videos are made from frames, where each frame is an image with a compressed format;.
- As each video consisting of its own number of frames decided by the size of the video, whenever converting the video to frames, the frames requires more memory than that of the original video.
- The surveillance video is composed of a sequence of group of pictures.

(b) ROI Extraction

- The ROIs containing privacy sensitive information such as faces are extracted through the ROI detection and segmentation methods.
- It's possible that there are more than one ROI in a video frame.
- LCA-based lightweight encryption algorithm is performed on every ROI to make the privacy sensitive information unrecognizable.,
- ROIs from a frame are encrypted independently.

(c) ROI Encryption

- Extracted ROI parts are encrypted with help of ECC encryption algorithm.
- Whereas the encrypted ROIs are stored at the server side.
- The stored ROI will be transmitted, decrypted to recover the original surveillance video.
- The ROIs encryption and the new video's encoding are carried out independently, which make the proposed method can not only protect privacy information, but also meet the real-time requirement.

(d) Video Retrieval

- The decryption key is the same as the encryption key.
- The evolution rules represented by the sequence are the reverse rules of the ones used in the encryption.
- Thereafter, the inverse trans- formation was performed.

SECURITY AND PERFORMANCE ANALYSIS

Encryption calculation utilized for security assurance in observation video ought to be sufficiently secure to avoid assailants getting the protection data from the scrambled recordings. In our work, locales contain private data in edges are scrambled by our LCA-based methodology and the non-security areas will stay flawless. A few factual tests and estimations are utilized to break down the security of our methodology.

(A) Data Entropy

Data entropy is an essential estimation for the dimensions dispersion in a picture. The entropy of a picture I is defined as pursues:

$$H(I) = -\sum_{i}^{L} p(x_i) \log_2 p(x_i)$$

Where L is the quantity of dark dimensions, x_i is the i^{th} dim an incentive in the picture I, $p(x_i)$ is the event likelihood of x_i, and p_i $p(x_i)=1$.

The higher the entropy is,the more the dark dimensions near uniform circulation are. For a picture satisfies uniform conveyance, there are 256 dark dimensions with a similar event probability, accordingly the ideal entropy esteem is 8 and the entropy of an encoded picture ought to be way to deal with such an esteem. Table 3 demonstrates a correlation of the entropies of three dark pictures and their relating figure pictures encoded by our LCA-based technique and some l-------different strategies. In Table 3, the entropies of the pictures scrambled by our strategy are near the ideal esteem 8, which exhibits that our technique is superior to that of alternate strategies.

(B) Histogram

A picture histogram straightforwardly displays the factual qualities of the picture pixel values. Generally, the pixel estimations of the encoded pictures need to fulfill a uniform irregular conveyance.

(C) Relationship of Adjacent Pixels

Correlation trial of the neighboring pixels is an imperative factual technique to assess the dispersion and disarray of an encryption calculation. Scrambled pictures ought to have a just about zero connection between's the neighboring pixels, though the plain pictures should display a solid relationship. To play out a connection test on a picture, we haphazardly pick 1,000 pairs of adjacent pixels in vertical, diagonal and horizontal directions from a plain image and its cipher image, separately. We at that point compute the relationship coefficient, where the connection coefficient is defined as pursues:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x).\sqrt{D(y)}}}$$

$$D(x) = \frac{1}{n}\sum_{i=1}^{n}\left(x_i - E(x)\right)^2$$

$$E(x) = \frac{1}{n}\sum_{i=1}^{n} x_i$$

$$cov(x,y) = \frac{1}{n}\sum_{i=1}^{n}(x_i - E(x))(y_i - E(y))$$

(D) Differential Analysis

A differential analysis refers to the influence of slight change in plain picture concerning the figure picture. In the event that a solitary pixel's change can have a significant influence in the figure picture, that the encryption calculation is secure against the differential assault is finished up. Two lists are utilized to quantify such an influence in

the paper, viz., the number of pixels change rate (NPCR) and the unified normal evolving power (UACI), where:

$$NPCR = \frac{\Sigma_{i,j} D(i,j)}{M \times N} \times 100\%$$

$$UACI = \frac{1}{M \times N} \sum_{i,j} \frac{[C_1(i,j) - C_2(i,j)]}{255} \times 100\%$$

$$D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j) \\ 1, & otherwise \end{cases}$$

(E) Key Sensitivity

As indicated by Shannon's hypothesis, encryption result should be delicate to any adjustments in a key. In our calculation, the key is made up of a pseudo random binary sequence and an iteration number. To test the key's affectability, the accompanying analyses are performedona 64×64 bits grayimage 'rice', viz., Fig.10(a). We first encoded the picture with K0(PR,N = 5) to get a reference figure picture C0, where PR is a 16 × 64 bits twofold succession, and after that we encode the plain picture with two modified keys K1(PR1,N = 5) and K2(PR,N = 7), where the contrast among PR and PR1 is just a single piece. The comparing figure pictures are signified by C1 and C2 respectively, as shown in Fig.10. In order to present a quantitative illustration, correlation co-efficients between C0 and C1, C0 and C2 are calculated. The values are −0.0196 and 0.0021, respectively, which show that our LCA-based approach is key delicate.

(F) Animal Force Attack

Animal power assault or thorough assault is an essential system of attempting each conceivable key thusly until the right key is identified. Hypothetically, the extent of the key space decides the down to earth practicality of playing out a savage power assault.

Note that a casing may has more than one RoIs. So as to lessen the expense of the key's circulation, all RoI obstructs in a casing will be encoded with a similar key. Since our methodology satisfies the necessities of perplexity and dispersion, regardless of whether two squares which have minor contrasts are encoded by a similar key, the outcomes are far various. Further more, a RoI extracted from a frame may be the same as the one from the other frames, those frames will be encrypted by various keys and thus even similar RoI will demonstrate diverse encryption results. Accordingly, it's computationally infeasible to dispatch a key beast drive assault to our methodology.

(G) Execution Analysis

Since CA are locally parallel, CA-based encryption plot is very efficient in both equipment and programming executions. In the lightweight LCA-based iterative picture encryption technique proposed, every cell performs rule evolution, transposition and XOR operations for N cycles, the computational multifaceted nature is O(N). The aftereffects of the execution examination demonstrated that it is more efficient when contrasted and some 1D and 2D based encryption strategies. In our LCA-based method, fewer operations are performed for every cell in all RoI hinders than the one. Just a single guideline advancement and three move changes are engaged with each iteration. For N iterations, the computational complexity of our technique is O(N), as well. Since the RoIs in each casing are composed into squares and be encoded freely and synchronously, which add to the

efficiency of our approach. Further more, the results of the above analysis show that even less cycle rounds empower the scrambled squares to have a decent factual trademark.

TEST RESULTS

The investigations dependent on the observation recordings of H.264, as showe din Fig.5(a) and (b), where the RoIs contain privacy delicate data, for example, human face and vehicle plate number. In our tests, the RoIs are removed by the strategy. The proposed methodology is connected on these extricated RoIs, the encoded RoIs are appeared in Fig. 5(c) and (d), the non privacy locales are then incorporated with the substitution districts (white area) for security assurance are appeared in Fig. 5 (e) and (f) and the recouped total video outlines for the verified clients are appeared in Fig. 5 (g) and (h).

CONCLUSION

Proposed approach of video encryption provides more secure communication and video transaction between sender and receiver. The proposed method satisfies the real-time requirements of secure data and videos sharing.

REFERENCES

[1] Auer, S., Bliem, A., Engel, D., Uhl, A., and Unterweger, A., (2013) "Bitstream-based JPEG Encryption in Real-time". *International Journal of Digital Crime and Forensics (IJDCF), 5* (3), pp. 1 – 14.

[2] Kanso, A., and Ghebleh, M., (2012) "A novel image encryption algorithm based on a 3D chaotic map". *Communications in Nonlinear Science and Numerical Simulation, 17* (7), pp. 2943 – 2959. DOI: https://doi.org/10.1016/j.cnsns.2011.11.030.

[3] Dufaux, F., (2011) *"Video scrambling for privacy protection in video surveillance: recent results and validation framework"*. Proceedings of SPIE - The International Society for Optical Engineering 8063. DOI: https://doi.org/10.1117/12.883948.

[4] Tralic, D., and Grgic, S., (2016) "Robust Image Encryption Based on Balanced Cellular Automaton and Pixel Separation". *Radioengineering, 25* (3), pp. 548 – 555.

[5] Chai, X., Gan, Z., Yuan, K., Chen, Y., and Liu, X., (2017) "A novel image encryption scheme based on DNA sequence operations and chaotic systems". *Neural Computing and Applications, 31*(1), pp. 219–237. DOI: https://doi.org/10.1007/s00521-017-2993-9.